

Protocol Sequences for Multiple-Packet Reception

Yijin Zhang, Yuan-Hsun Lo, Feng Shu and Wing Shing Wong

Abstract

Consider a time slotted communication channel shared by K active users and a single receiver. It is assumed that the receiver has the ability of the multiple-packet reception (MPR) to correctly receive at most γ ($1 \leq \gamma < K$) simultaneously transmitted packets. Each user accesses the channel following a specific periodical binary sequence, called the protocol sequence, and transmits a packet within a channel slot if and only if the sequence value is equal to one. The fluctuation in throughput is incurred by inevitable random relative shifts among the users due to the lack of feedback. A set of protocol sequences is said to be throughput-invariant (TI) if it can be employed to produce invariant throughput for any relative shifts, i.e., maximize the worst-case throughput. It was shown in the literature that the TI property without considering MPR (i.e., $\gamma = 1$) can be achieved by using shift-invariant (SI) sequences, whose generalized Hamming cross-correlation is independent of relative shifts. This paper investigates TI sequences for MPR; results obtained include achievable throughput value, a lower bound on the sequence period, an optimal construction of TI sequences that achieves the lower bound on the sequence period, and intrinsic structure of TI sequences. In addition, we present a practical packet decoding mechanism for TI sequences that incorporates packet header, forward error-correcting code, and advanced physical layer blind signal separation techniques.

The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Honolulu, HI, July 2014. This work was partially supported by the National Natural Science Foundation of China (No. 61301107, 61174060, 61271230), the Hong Kong RGC Earmarked Grant CUHK414012 and the Shenzhen Knowledge Innovation Program JCYJ20130401172046453.

Y. Zhang and F. Shu are with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. E-mail: yijin.zhang@gmail.com; shufeng@njust.edu.cn.

Y.-H. Lo is with the Department of Mathematics, National Taiwan Normal University, Taipei, Taiwan. E-mail: yhlo0830@gmail.com.

W. S. Wong is with the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N. T., Hong Kong. E-mail: wswong@ie.cuhk.edu.hk.

Index Terms

Collision channel without feedback, protocol sequences, multiple-packet reception, throughput.

I. INTRODUCTION

The idea of using *protocol sequences* to define deterministic multiaccess protocols for a collision channel without feedback was proposed by Massey and Mathys in [1], and recently has attracted many research revisits [2]–[7] for different design criteria and applications. Compared with time division multiple access (TDMA), ALOHA and carrier sense multiple access (CSMA), protocol sequences do not require stringent synchronization, channel monitoring, backoff algorithm and packet retransmissions. Such a simplicity is particularly desirable in ad hoc networks and sensor networks, in which well-coordinated transmissions and time synchronization may be difficult to achieve due to user mobility, time-varying propagation delays and energy constraints. Moreover, in contrast to the random and contention based schemes, protocol sequences in [2]–[7] can respectively provide a positive short-term throughput guarantee with probability one in the worst case.

Previous studies on multiaccess protocols have traditionally assumed a collision channel model of *single-packet reception* (SPR), in which a packet is received correctly only if it is not involved in a collision, i.e., does not overlap with another. However, the assumption of SPR becomes more and more unsuitable in practice, due to recent advances at reception techniques of the physical (PHY) layer, such as antenna arrays, CDMA technique and beamforming algorithms, which can be employed to ensure that the receiver has the ability of *multiple-packet reception* (MPR) [8] to receive multiple packets simultaneously. In this paper, we restrict our attention to protocol sequences for the γ -user MPR channel, in which a packet can be received error-free only if at most $\gamma - 1$ other packets are being transmitted simultaneously. We refer to γ as the *MPR capability* which has been commonly assumed in [9]–[13] for studying ALOHA and CSMA. However, it is expected that protocol sequences will also behave differently from what were reported in [2]–[7] for $\gamma = 1$ (i.e., SPR). Until only recently there has been no research published on protocol sequences for MPR. Only one related result [14] stated that there is no need of employing protocol sequences for a channel with a sufficiently large recovering probability of collided packets, which is different from the MPR capability discussed here.

The *effective throughput* of a user under the MPR capability γ is defined as the fraction of packets it can be sent out without suffering any collision in which more than γ users are involved. Due to a lack of feedback information, the relative shifts among users are unknown to each other, and thus incur performance variation in throughput. As argued in [5], [6], our main goal of designing protocol sequences is to maximize the worst-case individual throughput for any relative shifts, i.e., minimize the variation in throughput. If the throughput of each user is constant and independent of any relative shifts, then the assigned set of protocol sequences is said to be *throughput-invariant* (TI). It was shown in [1], [5], [6] that this zero-variance on throughput for $\gamma = 1$ can be achieved by using *shift-invariant* (SI) sequences, which enjoy the special property that their *generalized Hamming cross-correlation* is independent of relative shifts. The generalized Hamming cross-correlation here is a generalization of *pairwise Hamming cross-correlation* and defined for all nonempty subsets of users. However, the question of whether there exist TI sequences for $\gamma = 1$ which are shorter than SI sequences has not been answered. Moreover, the impact of MPR capability on the throughput performance and sequence design of TI sequences is not explored either. As such, this paper is a first attempt to study TI sequences for MPR, and can be viewed as a generalization of results in [6].

The remainder of this paper is organized as follows. After setting up the channel model and notation in Section II, we in Section III derive the throughput value of a system with MPR capability. In Section IV, lower bounds on the period of TI sequences with MPR capability are presented. In Section V, we use a known construction of SI sequences to design TI sequences for any MPR capability, which are optimal in the sense that the sequence period achieves the lower bound. Section VI proposes a mechanism of identification and decoding for TI sequences. It is further shown in Section VII that TI sequences must be SI in many specific cases, which indicates that the SI sequence set is the unique solution to the TI problem with MPR. Finally, in Section VIII we close the discussion with some concluding remarks.

II. CHANNEL MODEL AND NOTATION

Consider a time slotted communication channel shared by K active users and a single receiver. It is assumed that each of these users always has a fixed-length packet to send, knows the slot boundaries and transmits its packet within a channel slot. However, these users do not know the relative shifts of other users. Let τ_i , an integer measured in unit of slot duration, denote

the relative shift of user i for $i = 1, 2, \dots, K$. Following [1], we define a deterministic binary sequence, $\mathbf{s}_i := [s_i(0) \ s_i(1) \ \dots \ s_i(L-1)]$, called *protocol sequence* to schedule the packet transmission of user i for $i = 1, 2, \dots, K$, where L is the common sequence period of all K sequences. We consider that the channel is slot-synchronous so that there exists a system-wide slot labeling, t , and user i transmits a packet at slot t if $s_i(t + \tau_i) = 1$, and keeps silent if $s_i(t + \tau_i) = 0$, in which the addition by τ_i is in modulo L arithmetic.

Following the assumption of the γ -user MPR channel, we focus on the non-trivial case in which $\gamma < K$. A transmitted packet is correctly received if at most $\gamma - 1$ other packets are being transmitted at the same slot, and is considered lost otherwise. For practical considerations, the users can employ forward error-correcting code across packets to recover data lost, as explained in Section VI.

Some notation and definitions used in this paper are stated below.

Definition 1. For $i = 1, \dots, K$, define the duty factor f_i of a protocol sequence \mathbf{s}_i , as the fraction of ones in \mathbf{s}_i , namely,

$$f_i := \frac{1}{L} \sum_{t=0}^{L-1} s_i(t).$$

The cyclic shift of \mathbf{s}_i by τ_i is defined as

$$\mathbf{s}_i^{(\tau_i)} := [s_i(\tau_i) \ s_i(1 + \tau_i) \ \dots \ s_i(L - 1 + \tau_i)],$$

where the addition is taken modulo L . Note that the t -th bit of $\mathbf{s}_i^{(\tau_i)}$ is denoted by $s_i(t + \tau_i)$.

Definition 2. Let $b_j \in \{0, 1\}$ for $j = 1, \dots, K$. For a system with the MPR capability γ , the throughput of user i with the assigned sequence \mathbf{s}_i for given relative shifts τ_1, \dots, τ_K is defined as

$$R_i(\tau_1, \tau_2, \dots, \tau_K) = \frac{1}{L} \sum_{\substack{b_i=1, \\ q_i \leq \gamma-1}} N(b_1, \dots, b_K | \mathbf{s}_1^{(\tau_1)}, \dots, \mathbf{s}_K^{(\tau_K)}), \quad (1)$$

in which $q_i = \sum_{j \neq i} b_j$ and $N(b_1, \dots, b_K | \mathbf{s}_1^{(\tau_1)}, \dots, \mathbf{s}_K^{(\tau_K)})$ denotes the number of time indices t , $0 \leq t < L$, such that $s_j(t + \tau_j) = b_j$ for all j . This computes the fraction of time slots in which at most γ users including user i are transmitting. Note that the summation in (1) is taken over (b_1, \dots, b_K) with $b_i = 1, q_i \leq \gamma - 1$.

A sequence set $\{\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_K\}$ is said to be TI with the MPR capability γ if $R_i(\tau_1, \tau_2, \dots, \tau_K)$ is a constant function of $\tau_1, \tau_2, \dots, \tau_K$ for any i . For simplicity, we sometimes use R_i to denote

the throughput of user i . To avoid the uninteresting cases, in this paper we only consider TI sequences that ensure R_i is strictly bigger than zero for any i .

Definition 3. We identify the K users by means of the index set

$$\mathcal{K} := \{1, 2, \dots, K\}.$$

Let \mathcal{O}_K be the set

$$\bigcup_{n=1}^K \{(i_1, \dots, i_n) \in \mathcal{K}^n : i_1 < i_2 < \dots < i_n\}.$$

An element in \mathcal{O}_K corresponds to an ordered tuple of users. For $\mathbf{A} = (i_1, i_2, \dots, i_n) \in \mathcal{O}_K$, the generalized Hamming cross-correlation associated with \mathbf{A} is defined as

$$H(\tau_{i_1}, \dots, \tau_{i_n}; \mathbf{A}) := \sum_{t=0}^{L-1} \prod_{j=1}^n s_{i_j}(t + \tau_{i_j}).$$

If $|\mathbf{A}| = 2$, the generalized Hamming cross-correlation is reduced to the pairwise Hamming cross-correlation function.

We further introduce the following definitions by means of the generalized Hamming cross-correlation:

- (i) Given an ordered tuple $\mathbf{A} \in \mathcal{O}_K$, then $H(\tau_{i_1}, \dots, \tau_{i_n}; \mathbf{A})$ is said to be SI if it is a constant for any $\tau_{i_1}, \dots, \tau_{i_n}$.
- (ii) A sequence set is said to be SI [6] if $H(\tau_{i_1}, \dots, \tau_{i_n}; \mathbf{A})$ is SI for every \mathbf{A} in \mathcal{O}_K .
- (iii) A sequence set is said to be pairwise SI [15] if $H(\tau_{i_1}, \dots, \tau_{i_n}; \mathbf{A})$ is SI for every \mathbf{A} in \mathcal{O}_K with $|\mathbf{A}| = 2$.

III. THROUGHPUT OF TI SEQUENCES

Let $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_n$ be n binary sequences with a common period L . For $b_1, \dots, b_n \in \{0, 1\}$, Shum et al. [6] showed that

$$\sum_{\tau_1=0}^{L-1} \dots \sum_{\tau_n=0}^{L-1} N(b_1, \dots, b_n | \mathbf{s}_1^{(\tau_1)}, \dots, \mathbf{s}_n^{(\tau_n)}) = L \prod_{i=1}^n N(b_i | \mathbf{s}_i). \quad (2)$$

The main result in this section is summarized in the following.

Theorem 4. Let $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_K$ be K TI sequences with the MPR capability γ , $1 \leq \gamma < K$, and duty factors f_1, f_2, \dots, f_K respectively. Then we have

$$R_i = f_i \sum_{\substack{\mathbf{H} \subseteq \mathcal{K} \setminus \{i\} \\ |\mathbf{H}| < \gamma}} \prod_{j \in \mathbf{H}} f_j \prod_{k \in \mathcal{K} \setminus (\{i\} \cup \mathbf{H})} (1 - f_k). \quad (3)$$

Proof: Suppose that the relative shifts of \mathbf{s}_i is τ_i , for $i = 1, 2, \dots, K$. We can treat $\tau_1, \tau_2, \dots, \tau_K$ as independent and uniformly distributed random variables that are equally likely to take on any of L values: $0, 1, \dots, L - 1$. After taking the expectation over $(\tau_1, \tau_2, \dots, \tau_K)$, we obtain the average throughput of user i as the following:

$$\begin{aligned} & \mathbb{E}\left(R_i(\tau_1, \tau_2, \dots, \tau_K)\right) \\ &= \frac{1}{L} \mathbb{E}\left(\sum_{q_i \leq \gamma-1, b_i=1} N(b_1, \dots, b_K | \mathbf{s}_1^{(\tau_1)}, \dots, \mathbf{s}_K^{(\tau_K)})\right) \end{aligned} \quad (4)$$

$$\begin{aligned} &= \frac{1}{L} \sum_{q_i \leq \gamma-1, b_i=1} \mathbb{E}\left(N(b_1, \dots, b_K | \mathbf{s}_1^{(\tau_1)}, \dots, \mathbf{s}_K^{(\tau_K)})\right) \\ &= \frac{1}{L} \sum_{q_i \leq \gamma-1, b_i=1} \frac{1}{L^{K-1}} \prod_{j=1}^K N(b_j | \mathbf{s}_j) \end{aligned} \quad (5)$$

$$\begin{aligned} &= \frac{1}{L^{K-1}} \sum_{q_i \leq \gamma-1} \frac{N(1 | \mathbf{s}_i)}{L} \prod_{j=1, j \neq i}^K N(b_j | \mathbf{s}_j) \\ &= \frac{1}{L^{K-1}} f_i \sum_{q_i \leq \gamma-1} \prod_{j=1, j \neq i}^K N(b_j | \mathbf{s}_j) \\ &= f_i \sum_{\substack{\mathbf{H} \subseteq \mathcal{K} \setminus \{i\} \\ |\mathbf{H}| < \gamma}} \prod_{j \in \mathbf{H}} f_j \prod_{k \in \mathcal{K} \setminus (\{i\} \cup \mathbf{H})} (1 - f_k), \end{aligned}$$

where $q_i = \sum_{j \neq i} b_j$. (4) directly follows from (1), while (5) is due to (2). Furthermore, since $R_i(\tau_1, \dots, \tau_K)$ is a constant function of τ_1, \dots, τ_K , it must be equal to its average value. This completes the proof. \blacksquare

Note that Theorem 4 is a generalization of [6, Thm. 3], which focuses on the case of $\gamma = 1$.

For the symmetric case that each user has the same duty factor f , all users have the same throughput:

$$\sum_{j=0}^{\gamma-1} \binom{K-1}{j} f^{j+1} (1-f)^{K-1-j}. \quad (6)$$

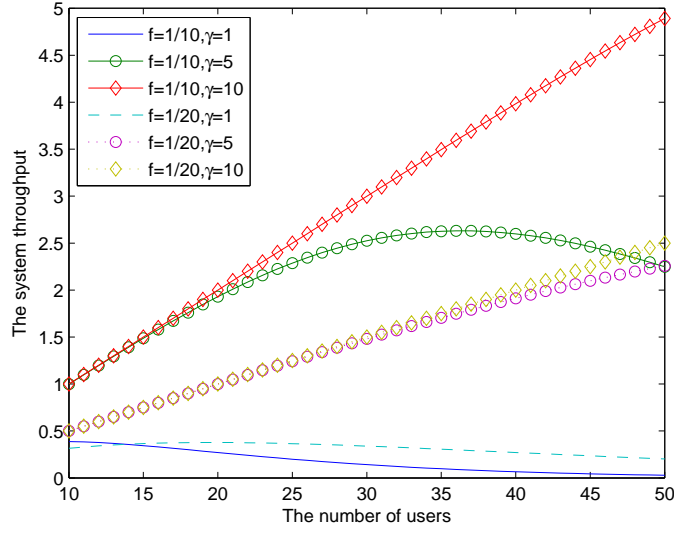


Fig. 1. The symmetric system throughput for $10 \leq K \leq 50$.

The system throughput in the symmetric case is plotted in Fig. 1 for $10 \leq K \leq 50$ with $\gamma = 1, 5, 10$ and $f = 1/10, 1/20$, respectively. We can see from (6) that there is an optimal duty factor for maximizing the throughput of a given user number. For $\gamma = 1$ the optimal value is $1/K$, but for the other cases the closed-form expression is difficult to obtain. See numerical results of optimal f in Fig. 2 for $K = 20$ and $\gamma = 1, 2, 3, 5, 8, 10, 12, 15$.

IV. LOWER BOUND ON MINIMUM PERIOD

A long sequence period could result in large variation in throughput on a short-time scale. With a weak assumption on duty factors, we derive lower bounds on the period of TI sequences for any γ in this section. These are clearly constraints on constructing TI sequences for small L values. Let $\gcd(x, y)$ denote the greatest common divisor of integers x and y .

Definition 5. Consider K binary sequences s_1, s_2, \dots, s_K with a common period L . Given an ordered tuple $A = (i_1, \dots, i_M) \in \mathcal{O}_K$ and relative shifts $\tau_{i_1}, \dots, \tau_{i_M}$ for some $M \leq K$, let $\theta_j(\tau_{i_1}, \dots, \tau_{i_M}; A)$, for $j = 0, 1, \dots, M$, denote the number of time indices t , $0 \leq t < L$, such

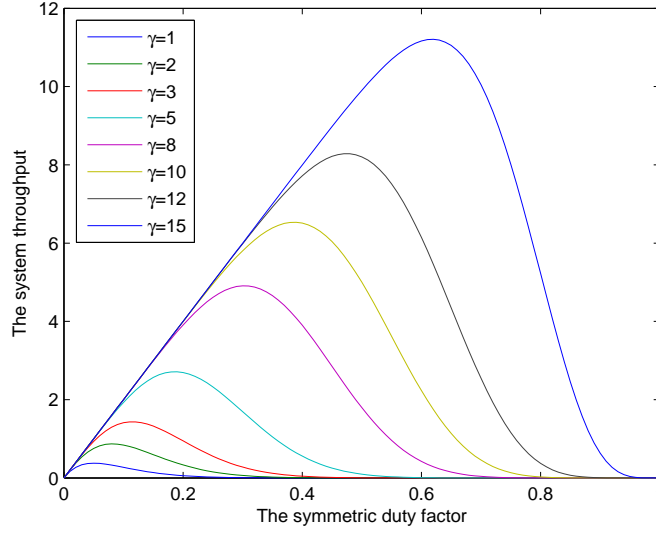


Fig. 2. The symmetric system throughput for $K = 20$ and different γ .

that there are exactly j '1's among $s_{i_1}(t + \tau_{i_1}), \dots, s_{i_M}(t + \tau_{i_M})$. Then, define

$$\theta_{\leq j}(\tau_{i_1}, \dots, \tau_{i_M}; \mathbf{A}) = \sum_{k=0}^j \theta_k(\tau_{i_1}, \dots, \tau_{i_M}; \mathbf{A}).$$

Note that $\theta_M(\tau_{i_1}, \dots, \tau_{i_M}; \mathbf{A}) = H(\tau_{i_1}, \dots, \tau_{i_M}; \mathbf{A})$.

Proposition 6. Consider a set of K sequences which is TI with the MPR capability γ ($1 \leq \gamma < K$). If $R_i > 0$ for any i , then there are at most $\gamma - 1$ all-one sequences.

Proof: Suppose there are γ all-one sequences. Then all packets from other $K - \gamma$ sequences cannot be received error-free. It implies $R_i = 0$ for some i , which contradicts the assumption. ■

Theorem 7. Let γ be any integer with $1 \leq \gamma < K$. If a set of K binary sequences is TI with the MPR capability γ , then this sequence set is pairwise SI.

Proof: Denote by $\mathbf{s}_1, \dots, \mathbf{s}_K$ the K sequences. The proof of the case $K = 2$ is straightforward. For $K > 2$, we aim to show that $\theta_2(\tau_{i_1}, \tau_{i_2}; \mathbf{A})$ is a constant function of τ_{i_1}, τ_{i_2} for any $\mathbf{A} = (i_1, i_2) \in \mathcal{O}_K$. Without loss of generality, let $\mathbf{A} = (1, 2)$, and let $\mathbf{B} = (3, \dots, K)$. That is, we divide these K sequences into two parts: $\mathcal{A} = \{\mathbf{s}_1, \mathbf{s}_2\}$ and $\mathcal{B} = \{\mathbf{s}_3, \dots, \mathbf{s}_K\}$.

First, we fix the relative shifts $\tau_3^*, \dots, \tau_K^*$ of sequences in \mathcal{B} such that $\theta_{\gamma-1}(\tau_3^*, \dots, \tau_K^*; \mathbf{B}) > 0$. This combination of relative shifts can always be found since there are at most $\gamma - 1$ all-one sequences in \mathcal{B} for the case $1 \leq \gamma < K$ following Proposition 6. Suppose in \mathcal{B} that there are exactly h all-one sequences. As $h \leq \gamma - 1 \leq K - 2$, then we cyclically shift some $\gamma - h - 1$ sequences which are not all-ones such that the first time slot of them are all equal to one, and cyclically shift the remaining $K - \gamma - 1$ sequences such that the first time slot of them are all equal to zero. Hence there are exactly $\gamma - 1$ ones in the first time slot.

For τ_1, τ_2 , we define

$$T_1(\tau_1, \tau_2) := \sum_{\substack{b_1+b_2=1 \\ b_3+\dots+b_K < \gamma}} N(b_1, \dots, b_K | \mathbf{s}_1^{(\tau_1)}, \mathbf{s}_2^{(\tau_2)}, \mathbf{s}_3^{(\tau_3^*)}, \dots, \mathbf{s}_K^{(\tau_K^*)})$$

and

$$T_2(\tau_1, \tau_2) := \sum_{\substack{b_1+b_2=2 \\ b_3+\dots+b_K < \gamma-1}} N(b_1, \dots, b_K | \mathbf{s}_1^{(\tau_1)}, \mathbf{s}_2^{(\tau_2)}, \mathbf{s}_3^{(\tau_3^*)}, \dots, \mathbf{s}_K^{(\tau_K^*)}).$$

We assume the relative shifts τ_1, τ_2 are uniformly distributed in $0, 1, \dots, L - 1$. After taking the expectation over τ_1, τ_2 , we have

$$\mathbb{E}(LR_1 + LR_2) = \mathbb{E}(T_1(\tau_1, \tau_2) + 2T_2(\tau_1, \tau_2)) = \mathbb{E}(T_1(\tau_1, \tau_2)) + 2\mathbb{E}(T_2(\tau_1, \tau_2)) \quad (7)$$

$$= \frac{1}{L} \sum_{i=1}^2 i \theta_i(\tau_1, \tau_2; \mathbf{A}) \theta_{\leq \gamma-i}(\tau_3^*, \dots, \tau_K^*; \mathbf{B}). \quad (8)$$

The proof of (8) is relegated to Appendix A.

We now change the pair of relative shifts from (τ_1, τ_2) to (τ'_1, τ'_2) . Let

$$\sigma := \theta_2(\tau'_1, \tau'_2; \mathbf{A}) - \theta_2(\tau_1, \tau_2; \mathbf{A}). \quad (9)$$

By the fact that

$$\theta_1(\tau_1, \tau_2; \mathbf{A}) + 2\theta_2(\tau_1, \tau_2; \mathbf{A}) = Lf_1 + Lf_2 = \theta_1(\tau'_1, \tau'_2; \mathbf{A}) + 2\theta_2(\tau'_1, \tau'_2; \mathbf{A}),$$

we have

$$\theta_1(\tau'_1, \tau'_2; \mathbf{A}) - \theta_1(\tau_1, \tau_2; \mathbf{A}) = -2\sigma. \quad (10)$$

Since $R_1 + R_2$ has zero-variance, by (7) and (8), we have

$$\begin{aligned} & \sum_{i=1}^2 i \theta_i(\tau_1, \tau_2; \mathbf{A}) \theta_{\leq \gamma-i}(\tau_3^*, \dots, \tau_K^*; \mathbf{B}) \\ &= \sum_{i=1}^2 i \theta_i(\tau'_1, \tau'_2; \mathbf{A}) \theta_{\leq \gamma-i}(\tau_3^*, \dots, \tau_K^*; \mathbf{B}). \end{aligned}$$

Then it follows from (9) and (10) that

$$\sigma \theta_{\gamma-1}(\tau_3^*, \dots, \tau_K^*; \mathbf{B}) = 0,$$

which implies that $\sigma = 0$ because of $\theta_{\gamma-1}(\tau_3^*, \dots, \tau_K^*; \mathbf{B}) > 0$ due to the choice of $\tau_3^*, \dots, \tau_K^*$.

Thus, $\theta_2(\tau_1, \tau_2; \mathbf{A})$ is a constant function of τ_1, τ_2 .

Since $\theta_2(\tau_1, \tau_2; \mathbf{A}) = H(\tau_1, \tau_2; \mathbf{A})$ and the choice of \mathbf{A} is arbitrary, we conclude that a set of these K sequences is pairwise SI for any $\gamma < K$. ■

Compared with the SI property which has been proved as a sufficient condition of a sequence set being TI for $\gamma = 1$ [6], pairwise SI is conceptually a weaker requirement on sequence design. However, they are known to enjoy the same lower bound on the minimum sequence period for some special form of duty factors. Given any set of K pairwise SI sequences with duty factors n_i/d_i , where $\gcd(n_i, d_i) = 1$ for all i , Zhang et al. [15, Thm. 1] proved that its common period is divisible by $d_1 d_2 \cdots d_K$. By Theorem 7, we then have the following result.

Corollary 8. *Let γ be an integer with $1 \leq \gamma < K$. If a set of K binary sequences with duty factors n_i/d_i , where $\gcd(n_i, d_i) = 1$ for all i , is TI with the MPR capability γ , then its common period is divisible by $d_1 d_2 \cdots d_K$. In particular, the minimum common period is at least $d_1 d_2 \cdots d_K$.*

With duty factors n_i/d_i where $\gcd(n_i, d_i) = 1$ for all i , Corollary 8 further obtains that the lower bound on the period of TI sequences still grows exponentially with K for any γ , although their combinatorial design requirement is different from that of pairwise SI and SI sequences.

V. AN OPTIMAL CONSTRUCTION

Shum et al. [6] showed that any SI sequence set is TI for the classical model ($\gamma = 1$). In this section, we extend this property to general γ by means of the following result.

Theorem 9 ([6, Thm. 1]). *The sequence set $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_K$ is SI if and only if for each choice of b_1, \dots, b_K , $N(b_1, \dots, b_K | \mathbf{s}_1^{(\tau_1)}, \dots, \mathbf{s}_K^{(\tau_K)})$ is a constant function of τ_1, \dots, τ_K .*

Theorem 10. *If a sequence set is SI, then it is TI for any MPR capability γ .*

Proof: From (1), we obtain the result that the throughput $R_i(\tau_1, \tau_2, \dots, \tau_K)$ can be computed only in terms of $N(b_1, \dots, b_K | \mathbf{s}_1^{(\tau_1)}, \dots, \mathbf{s}_K^{(\tau_K)})$ for some particular choices of b_1, \dots, b_K . By

Theorem 9, we find each term of the above is a constant function of τ_1, \dots, τ_K if the sequence set is SI. Thus $R_i(\tau_1, \tau_2, \dots, \tau_K)$ is also a constant function of τ_1, \dots, τ_K , which implies that a SI sequence set must be TI for any γ . ■

Theorem 10 implies that we can use known constructions of SI sequences to design TI sequences for any MPR capability γ . A general construction of SI sequences was given in [6], and we present it here for the sake of completeness. The proof that the sequences so generated are SI can be found in [6].

An optimal construction [6]. Given the duty factors $n_1/d_1, n_2/d_2, \dots, n_K/d_K$ where $\gcd(n_i, d_i) = 1$ for all i , we construct \mathbb{G}_i , a $\prod_{j=1}^{i-1} d_j \times d_i$ array of zeros and ones such that there are exactly n_i ones in each row. ($\prod_{j=1}^0 d_j$ is defined as 1, as the empty product is equal to 1 by convention.) Then construct s_i by reading out the columns of this array from left to right and extending them periodically to the period $d_1 d_2 \cdots d_K$, for $i = 1, 2, \dots, K$.

It is shown that this construction produces the common period $d_1 d_2 \cdots d_K$ for all K sequences, and thus it is *an optimal construction of TI sequences* for any γ when $\gcd(n_i, d_i) = 1$ for all i , in the sense that the period achieves the lower bound in Corollary 8.

Example: Given the duty factors $f_1 = 2/3$ and $f_2 = f_3 = 1/3$, we can obtain the following three zero-one arrays by the above construction.

$$\mathbb{G}_1 = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}, \quad \mathbb{G}_2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad \mathbb{G}_3 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

Then we read out the columns of \mathbb{G}_i from left to right and extend them periodically to s_i of

length 27, for $i = 1, 2, 3$.

$$\mathbf{s}_1 = [1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0]$$

$$\mathbf{s}_2 = [1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0]$$

$$\mathbf{s}_3 = [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$$

One can check that, for all τ_1, τ_2 and τ_3 , the values of the generalized Hamming cross-correlations are $H(\tau_1, \tau_2; (1, 2)) = 6$, $H(\tau_2, \tau_3; (2, 3)) = 3$, $H(\tau_1, \tau_3; (1, 3)) = 6$ and $H(\tau_1, \tau_2, \tau_3; (1, 2, 3)) = 2$. Hence the sequence set is SI. It can produce invariant individual throughput for any MPR capability and thus is also TI. We have $R_1 = 8/27, R_2 = R_3 = 1/27$ for $\gamma = 1$ and $R_1 = 16/27, R_2 = R_3 = 7/27$ for $\gamma = 2$ which are both in accordance with Theorem 4. Its period is 27 which achieves the lower bound presented in Corollary 8 for $\gamma = 1, 2$.

We furthermore present a numerical evaluation of the throughput performance of the TI sequences produced by the SI construction. A symmetric and saturated system with the MPR capability γ is considered. We conduct 10^5 simulation runs for each K, γ to generate 10^5 combinations of uniformly distributed relative shifts. Similar to [6] for $\gamma = 1$, in order to examine the throughput variation and average throughput over the sequence period, TI sequences with the duty factor $1/K$ are compared with a random access scheme in which a user sends a packet in each slot with an independent probability $1/K$. In Fig. 3, we plot the maximum, mean and minimum individual throughput for $\gamma = 2, 3$ with $\gamma < K \leq 7$. TI sequences yield constant symmetric individual throughput as derived in (6). For the random access scheme, the mean throughput is equal to that of TI sequences as expected; the maximum and minimum throughput are getting closer when the averaging time scale increases, due to the strong law of large numbers. Results have shown that the SI construction can provide zero-variance on throughput for MPR.

VI. IDENTIFICATION AND DECODING

In a protocol sequences based multiaccess protocol, the receiver needs to accomplish the following two tasks [2]–[4]:

- (i) identify the sender of each successfully received packet (the *identification problem*);
- (ii) decode each successfully received packet and recover the original information (the *decoding problem*).

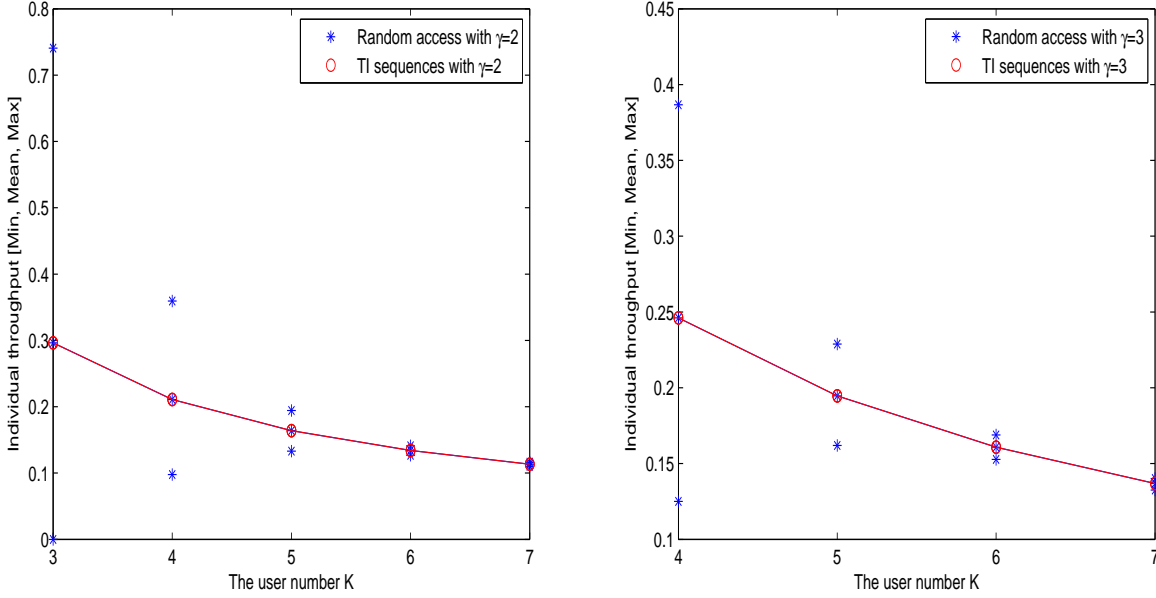


Fig. 3. The minimum, mean, and maximum individual throughput from simulation for $\gamma = 2, 3$ with $\gamma < K \leq 7$. The mean value is connected by a piece-wise linear curve. The symbols above and below this curve indicate the maximum and minimum value, respectively.

Merely relying on some special structure of SI sequences, Shum et al. in [6] generalized the *decimation algorithm* [1], [16] to solve the identification problem of all uncollided packets without the need of using header information. However, this solution is invalid for packets survived in collisions if MPR is considered for $\gamma > 1$.

The problem of packet separation at the PHY layer with MPR is usually formulated as signal separation in a *multiple-input-multiple-output* (MIMO) system. Let $x_i(n)$ denote the symbol transmitted by user i in symbol duration n , $\mathbf{w}(n)$ denote the additive noise, and $\mathbf{h}_i(n)$ denote the user i 's channel vector in symbol duration n . The vector $\mathbf{h}_i(n)$ depends on the configuration of channel diversity, for example, in a multiple antenna system its m th element represents the channel coefficient from user i to the m -th receive antenna. Suppose that the users i_1, i_2, \dots, i_M are transmitting simultaneously in symbol duration n , and then the received signal at the receiver

in symbol duration n is given by

$$\begin{aligned}\mathbf{y}(n) &= \sum_{j=1}^M \mathbf{h}_{i_j}(n)x_{i_j}(n) + \mathbf{w}(n) \\ &= \mathbf{H}(n)\mathbf{x}(n) + \mathbf{w}(n),\end{aligned}$$

where $\mathbf{H}(n) = [\mathbf{h}_{i_1}(n), \mathbf{h}_{i_2}(n), \dots, \mathbf{h}_{i_M}(n)]$, $\mathbf{x}(n) = [x_{i_1}(n), x_{i_2}(n), \dots, x_{i_M}(n)]^T$. The problem of signal separation here is how to estimate transmitted symbols $\mathbf{x}(n)$ from the received vector $\mathbf{y}(n)$, when at most γ users are transmitting simultaneously, i.e., $M \leq \gamma$. It is unrealistic to assume that the receiver knows the channel vector $\mathbf{H}(n)$, and thus various training-based signal separation algorithms have been developed in the literature for the estimation of $\mathbf{H}(n)$, which requires that the receiver has priori knowledge of the senders' identities, the training sequences and their locations in a packet. However, these algorithms cannot be applied in protocol sequences based multiaccess, because that the transmitting users are changing and unknown to the receiver due to the random relative shifts of the users.

To address these problems, this section proposes a mechanism of the identification and decoding for TI sequences considering $\gamma > 1$, as below.

- (a) Each packet contains a header that indicates the user identity and packet identity. This is also a common practice in protocol sequences systems [4], [7]. Note that the packet identity only has one bit information which denotes whether this packet is transmitted in an odd period (the period order number module 2 equals 1). The bit size of such a header can be found as $1 + \log_2 K$, so its effect on the system performance is negligible.
- (b) For those collision slots occupied by at most γ transmitting users, one can find out the packet content by employing blind signal separation algorithms [17]–[19], which can obtain $\mathbf{x}(n)$ from $\mathbf{y}(n)$ without knowing who are the senders and $\mathbf{H}(n)$ in advance. Interested readers are referred to [17], [18] for more details at the signal processing level. The complexity of the separation algorithm here depends on γ , since γ is the maximum dimension of $\mathbf{x}(n)$. Note that such an idea was also adopted in [9] for packet separation in IEEE 802.11 with MPR.
- (c) As mentioned in [1], [4], [7], we apply a Reed-Solomon (RS) code across the data payloads in a period to jointly code and decode the original information even if some packets are unavoidably lost, provided that the required minimum number of survived packets in each

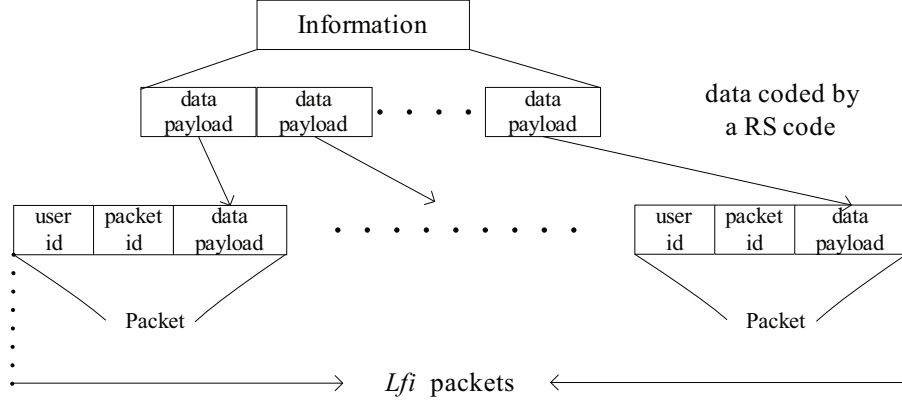


Fig. 4. Packet format using RS code of user i with the duty factor f_i for $i = 1, 2, \dots, K$.

period of a user is equal to or smaller than that guaranteed by TI sequences derived in Section III. The receiver knows which packets are transmitted in the same sequence period through the packet identity.

An illustration of the packet format and RS code is given in Fig. 4. By using TI sequences, we ensure that in each sequence period there are enough time slots in which the packets can be separated. Moreover, by using the embedded user identity and packet identity, the receiver can further recover enough fragments of the coded data to decode the original information.

One sees that all approaches mentioned above have been commonly employed in protocol sequences for $\gamma = 1$ and contention based network for $\gamma > 1$. Therefore, our mechanism does not cause any additional burden on system performance and receiver design, compared with other MPR protocols.

VII. STRUCTURAL THEOREM

It was proved in [6] that the period of K SI sequences with the duty factors $f_i = n_i/d_i$ for $i = 1, 2, \dots, K$ must be divisible by

$$\frac{\prod_{i \in \mathcal{U}} d_i}{\gcd(\prod_{i \in \mathcal{U}} d_i, \prod_{i \in \mathcal{U}} n_i)}, \quad (11)$$

for any subset \mathcal{U} of \mathcal{K} .

Given that SI sequences possess the TI property for any MPR capability and suffer from the drawback that the common period grows exponentially with K as shown in (11), a natural

question is whether there are shorter TI sequences, as a smaller period is favorable in practical applications. Unfortunately, results we have attained in Section IV rule this out for any γ under the assumption that $\gcd(n_i, d_i) = 1$ in $f_i = n_i/d_i$ for all i . However, there is no definite proof yet that the lower bound on the minimum period of TI sequences grows exponentially. So technically it is of interest to know more about the structure of TI sequences and resolve whether there exist TI sequences which are not SI. Results in Section VII can shed light in this direction.

The main objective of this section is to demonstrate that the SI property is intrinsic for TI sequences by proving TI implies SI for many specific cases. This tends to imply that there are no practical solutions to the TI problem with MPR. We may need to use wobbling sequences [4] or CRT sequences [7] instead. Although these sequences are not SI, their pairwise Hamming cross-correlation functions are close to being constant and they can guarantee a quasi-TI throughput performance on a relatively short time scale.

Define a k -subset as a set containing exactly k elements. We begin our study on the structural theorem with the following proposition.

Proposition 11. *Let γ be a positive integer smaller than K and $\mathcal{S} = \{\mathbf{s}_1, \dots, \mathbf{s}_K\}$ be a set of K binary sequences. If \mathcal{S} is TI with the MPR capability γ and any $(K - 1)$ -subset of \mathcal{S} is SI, then \mathcal{S} is SI.*

Proof: For a given set of relative shifts τ_1, \dots, τ_K , define a $K \times L$ matrix \mathbb{M} by putting $\mathbf{s}_i^{(\tau_i)}$ at the i -th row, for $i = 1, \dots, K$. By regarding an ordered tuple $\mathbf{A} \in \mathcal{O}_K$ as a subset of \mathcal{K} , the generalized Hamming cross-correlation $H(\tau_j : j \in \mathbf{A}; \mathbf{A})$ can be viewed as the number of all-one columns in the submatrix obtained by collecting all j -th row of \mathbb{M} , $j \in \mathbf{A}$. Notice that $LR_i(\tau_1, \dots, \tau_K)$ counts those ‘1’s on the i -th row such that the corresponding column-sum in \mathbb{M} does not exceed γ . By the principle of inclusion-and-exclusion, we have

$$\begin{aligned} LR_i(\tau_1, \dots, \tau_K) &= Lf_i - \sum_{i \in \mathbf{A}, |\mathbf{A}|=\gamma+1} H(\tau_j : j \in \mathbf{A}; \mathbf{A}) \\ &\quad + \sum_{i \in \mathbf{A}, |\mathbf{A}|=\gamma+2} H(\tau_j : j \in \mathbf{A}; \mathbf{A}) + \dots + (-1)^{K-\gamma} \sum_{i \in \mathbf{A}, |\mathbf{A}|=K} H(\tau_j : j \in \mathbf{A}; \mathbf{A}). \end{aligned}$$

Since $H(\tau_j : j \in \mathbf{A}; \mathbf{A})$ is SI for $|\mathbf{A}| < K$ and $R_i(\tau_1, \dots, \tau_K)$ has zero-variance by the condition, $H(\tau_j : j \in \mathcal{K}; \mathcal{K})$ is also SI. Therefore, $H(\tau_j : j \in \mathbf{A}; \mathbf{A})$ is SI for every \mathbf{A} in \mathcal{K} , which implies the entire sequence set \mathcal{S} is SI. ■

Definition 12. Consider M binary sequences $\mathbf{s}_1, \dots, \mathbf{s}_M$ with a common period. Let $\mathbf{M} = (1, \dots, M)$. Given two distinct systems of relative shifts $\tau = (\tau_1, \dots, \tau_M)$ and $\tau' = (\tau'_1, \dots, \tau'_M)$, let

$$\delta_i(\tau \rightarrow \tau'; \mathbf{M}) := \theta_i(\tau'_1, \dots, \tau'_M; \mathbf{M}) - \theta_i(\tau_1, \dots, \tau_M; \mathbf{M}),$$

denote the change of the value θ_i , for $i = 0, 1, \dots, M$.

Lemma 13. Consider M binary sequences $\mathbf{s}_1, \dots, \mathbf{s}_M$ with a common period and two distinct systems of relative shifts $\tau = (\tau_1, \dots, \tau_M)$ and $\tau' = (\tau'_1, \dots, \tau'_M)$. If any $(M - 1)$ -subset of $\{\mathbf{s}_1, \dots, \mathbf{s}_M\}$ is SI, then for $i = 1, \dots, M - 1$,

$$\delta_i(\tau \rightarrow \tau'; \mathbf{M}) = (-1)^{M-i} \binom{M}{i} \delta_M(\tau \rightarrow \tau'; \mathbf{M}). \quad (12)$$

Proof: In this proof we simply write δ_i instead of $\delta_i(\tau \rightarrow \tau'; \mathbf{M})$. For $j = 1, \dots, M - 1$, let Φ_j be a collection of all ordered pairs $(\mathbf{A}; t)$ with $|\mathbf{A}| = j$, $\mathbf{A} \in \mathcal{O}_M$, such that $s_i(t + \tau_i) = 1$ for each $i \in \mathbf{A}$. We shall count the cardinality of Φ_j in two ways. By the definition of θ_i , we have

$$|\Phi_j| = \sum_{i=j}^M \binom{i}{j} \theta_i(\tau_1, \dots, \tau_M; \mathbf{M}).$$

On the other hand, Φ_j computes all generalized Hamming cross-correlations among every j sequences. Then, we have

$$|\Phi_j| = \sum_{|\mathbf{A}|=j, \mathbf{A} \in \mathcal{O}_M} H(\tau_i : i \in \mathbf{A}; \mathbf{A}),$$

which is a constant function of τ_1, \dots, τ_j due to the assumption that each $(M - 1)$ -subset is SI. Therefore, we have

$$\sum_{i=j}^M \binom{i}{j} \theta_i(\tau_1, \dots, \tau_M; \mathbf{M}) = \sum_{i=j}^M \binom{i}{j} \theta_i(\tau'_1, \dots, \tau'_M; \mathbf{M})$$

and thus

$$\sum_{i=j}^M \binom{i}{j} \delta_i = 0. \quad (13)$$

Finally, the result follows by plugging $j = M - 1, M - 2, \dots, 1$ into (13) step by step. More precisely, from (13) we inductively have

$$\begin{aligned}
\delta_j &= -\binom{j+1}{j}\delta_{j+1} - \binom{j+2}{j}\delta_{j+2} - \dots - \binom{M}{j}\delta_M \\
&= (-1)^{M-j} \left[\binom{j+1}{1}\binom{M}{j+1} - \binom{j+2}{2}\binom{M}{j+2} + \dots + (-1)^{M-j-1}\binom{M}{M-j}\binom{M}{M} \right] \delta_M \\
&= (-1)^{M-j}\binom{M}{j} \left[\binom{M-j}{1} - \binom{M-j}{2} + \dots + (-1)^{M-j-1}\binom{M-j}{M-j} \right] \delta_M \\
&= (-1)^{M-j}\binom{M}{j}\delta_M,
\end{aligned}$$

as desired. ■

Lemma 14. *Let $\mathcal{S} = \{\mathbf{s}_1, \dots, \mathbf{s}_K\}$ be a set of K binary sequences with a common period L . Let $\mathbf{A} = (1, \dots, M)$, $\mathbf{B} = (M+1, \dots, K)$, for some $M < K$, and $\tau = (\tau_1, \dots, \tau_M)$, $\tau' = (\tau'_1, \dots, \tau'_M)$, $\tau^* = (\tau_1^*, \dots, \tau_M^*)$ be three systems of relative shifts. If \mathcal{S} is TI with the MPR capability γ and any $(M-1)$ -subset of \mathcal{S} is SI, then*

$$\delta_M(\tau \rightarrow \tau'; \mathbf{A}) \sum_{i=1}^{M-1} (-1)^{M-i} \binom{M-2}{i-1} \theta_{\gamma-i}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B}) = 0. \quad (14)$$

Note that $\theta_{\gamma-i}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B}) = 0$ if $\gamma < i$ or $\gamma - i > K - M$.

Proof: Let R_i be the individual throughput associated with \mathbf{s}_i . Similar to the arguments in (7) – (8), after taking the expectation over the relative shifts τ_1, \dots, τ_M , we have

$$\mathbb{E}(LR_1 + \dots + LR_M) = \sum_{i=1}^M \frac{i \theta_i(\tau_1, \dots, \tau_M; \mathbf{A}) \theta_{\leq \gamma-i}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B})}{L}, \quad (15)$$

which is a constant function of τ_1, \dots, τ_M due to the zero-variance of $R_1 + \dots + R_M$.

Now, consider that the relative shifts of the sequences $\mathbf{s}_1, \dots, \mathbf{s}_M$ are changed from τ to τ' . By Lemma 13 and (15), we have

$$\begin{aligned}
0 &= \sum_{i=1}^M \frac{i \delta_i(\tau \rightarrow \tau'; \mathbf{A}) \theta_{\leq \gamma-i}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B})}{L} \\
&= \frac{1}{L} \sum_{i=1}^M (-1)^{M-i} i \binom{M}{i} \delta_M(\tau \rightarrow \tau'; \mathbf{A}) \theta_{\leq \gamma-i}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B}) \\
&= \frac{\delta_M(\tau \rightarrow \tau'; \mathbf{A}) M}{L} \sum_{i=1}^M (-1)^{M-i} \binom{M-1}{i-1} \theta_{\leq \gamma-i}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B}).
\end{aligned}$$

Thus,

$$\delta_M(\tau \rightarrow \tau'; \mathbf{A}) \sum_{i=1}^M (-1)^{M-i} \binom{M-1}{i-1} \theta_{\leq \gamma-i}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B}) = 0. \quad (16)$$

Finally, the target identity (14) can be obtained from (16). See Appendix B for the derivation steps of (16) \Rightarrow (14). ■

The following result follows from the previous lemma.

Proposition 15. *Following the setting of Lemma 14, if all sequences have the same duty factor f , then*

$$\delta_M(\tau \rightarrow \tau'; \mathbf{A}) \sum_{i=1}^{M-1} (-1)^{M-i} \binom{M-2}{i-1} \binom{K-M}{\gamma-i} f^{\gamma-i} (1-f)^{K-M-\gamma+i} = 0.$$

Note that $\binom{K-M}{\gamma-i} = 0$ if $\gamma < i$ or $\gamma - i > K - M$.

Proof: Observe that there is no constraint on the choice of $\tau_{M+1}^*, \dots, \tau_K^*$ in (14). After taking the expectation over all possible relative shifts of $\mathbf{s}_{M+1}, \dots, \mathbf{s}_K$, we can replace the term $\theta_{\gamma-i}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B})$ in (14) by

$$\binom{K-M}{\gamma-i} f^{\gamma-i} (1-f)^{K-M-\gamma+i}.$$

This completes the proof. ■

We are ready for our main results in this section.

A. The case of $\gamma = 1$

Theorem 16. *Let $\mathcal{S} = \{\mathbf{s}_1, \dots, \mathbf{s}_K\}$ be a set of K binary sequences. If \mathcal{S} is TI with the MPR capability 1, then it is SI.*

Proof: We claim by induction that any M -subset of \mathcal{S} is SI for $M = 2, 3, \dots, K-1$. The case of $M = 2$ has been settled in Theorem 7, so we consider $M \geq 3$ and assume that any set of $M-1$ sequences is SI.

Without loss of generality, let $\mathbf{A} = (1, \dots, M)$ and $\mathbf{B} = (M+1, \dots, K)$. Let the relative shifts of $\mathbf{s}_1, \dots, \mathbf{s}_M$ be changed from $\tau = (\tau_1, \dots, \tau_M)$ to $\tau' = (\tau'_1, \dots, \tau'_M)$. Now, fix the relative shifts of $\mathbf{s}_{M+1}, \dots, \mathbf{s}_K$ be $\tau^* = (\tau_{M+1}^*, \dots, \tau_K^*)$ such that $\theta_0(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B}) > 0$. Such

τ^* is always existent because there is no all-one sequence in \mathcal{S} for $\gamma = 1$ following Proposition 6. By Lemma 14 ($\gamma = 1$), we have

$$\delta_M(\tau \rightarrow \tau'; \mathbf{A})\theta_0(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B}) = 0,$$

which implies that $\delta_M(\tau \rightarrow \tau'; \mathbf{A}) = 0$ due to the choice of τ^* . Therefore, $\theta_M(\tau_1, \dots, \tau_M; \mathbf{A})$ is a constant function of τ_1, \dots, τ_M , and thus $\{\mathbf{s}_1, \dots, \mathbf{s}_M\}$ is SI.

By induction on M from $M = 2$, we conclude that any $(K - 1)$ -subset of \mathcal{S} is SI. This furthermore implies that the entire set \mathcal{S} is SI from Proposition 11. \blacksquare

Theorem 16 asserts that SI and TI sequences are equivalent for $\gamma = 1$ (i.e., SPR).

B. The case of $\gamma = 2$

Theorem 17. *Let $\mathcal{S} = \{\mathbf{s}_1, \dots, \mathbf{s}_K\}$ be a set of K binary sequences with the same duty factor $f = \frac{n}{d} \neq 0, 1$, which is TI with the MPR capability 2. \mathcal{S} is SI if $\gcd(K - 2, d) = 1$.*

Proof: We claim by induction that any M -subset of \mathcal{S} is SI for $M = 2, 3, \dots, K - 1$. The case of $M = 2$ holds by Theorem 7, so we consider $M \geq 3$.

Similar to the proof of Theorem 16, let $\mathbf{A} = (1, \dots, M)$, $\mathbf{B} = (M + 1, \dots, K)$, $\tau = (\tau_1, \dots, \tau_M)$ and $\tau' = (\tau'_1, \dots, \tau'_M)$. By Proposition 15 ($\gamma = 2$), we have

$$\delta_M(\tau \rightarrow \tau'; \mathbf{A}) \left((K - M)f(1 - f)^{K-M-1} - (M - 2)(1 - f)^{K-M} \right) = 0.$$

By assuming $K \geq 3$, the above equation can be simplified to

$$\delta_M(\tau \rightarrow \tau'; \mathbf{A}) \left(f - \frac{M - 2}{K - 2} \right) = 0.$$

There are two cases.

- (a) $f = \frac{M-2}{K-2}$: If $\gcd(K - 2, d) = 1$, then $f = \frac{M-2}{K-2}$ contradicts to the assumption that $f = \frac{n}{d}$, and thus we have $\delta_M(\tau \rightarrow \tau'; \mathbf{A}) = 0$.
- (b) $\delta_M(\tau \rightarrow \tau'; \mathbf{A}) = 0$: This implies that $\theta_M(\tau_1, \dots, \tau_M; \mathbf{A})$ is a constant of τ_1, \dots, τ_M . Hence, $\{\mathbf{s}_1, \dots, \mathbf{s}_M\}$ is SI.

By induction on M from $M = 2$, we conclude that any $(K - 1)$ -subset of \mathcal{S} is SI. This furthermore implies that the entire set \mathcal{S} is SI from Proposition 11. \blacksquare

C. The case of $\gamma = 3$

Theorem 18. *Let $\mathcal{S} = \{\mathbf{s}_1, \dots, \mathbf{s}_K\}$ be a set of K binary sequences with the same duty factor $f = \frac{n}{d} \neq 0, 1$, which is TI with the MPR capability 3. Then \mathcal{S} is SI if (i) $K - 3$ is prime, and (ii) $\gcd(\frac{K-2}{2}, d) = 1$.*

Proof: The structure of this proof is similar to Theorems 16 and 17, so we only show the inductive step here.

Similar to the proof of Theorem 16, let $\mathbf{A} = (1, \dots, M)$, $\mathbf{B} = (M+1, \dots, K)$, $\tau = (\tau_1, \dots, \tau_M)$ and $\tau' = (\tau'_1, \dots, \tau'_M)$. By Proposition 15 ($\gamma = 3$), we have

$$\delta_M(\tau \rightarrow \tau'; \mathbf{A}) \left(\binom{K-2}{2} f^2 - (K-3)(M-2)f + \binom{M-2}{2} \right) = 0. \quad (17)$$

Suppose to the contrary that $\delta_M(\tau \rightarrow \tau'; \mathbf{A}) \neq 0$. If $M = 3$, since $K > M$ and $f \neq 0$, then (17) holds only when $f = \frac{2}{K-2}$, which contradicts to the assumption that $f = \frac{n}{d}$ and (ii) $\gcd(\frac{K-2}{2}, d) = 1$ ($\frac{K-2}{2}$ must be an integer as $K - 3$ is prime). If $M > 3$, (17) can be simplified to

$$\binom{p+1}{2} f^2 - p(M-2)f + \binom{M-2}{2} = 0, \quad (18)$$

where $p = K - 3$ is a prime number by (i). Since the duty factor f should be a rational number, the discriminant

$$D := p^2(M-2)^2 - p(p-1)(M-2)(M-3)$$

of the quadratic equation (18) is a square number. That is,

$$(M-2)(M-3) \equiv 0 \pmod{p}. \quad (19)$$

Since $M < K$, (19) holds only when $M - 2 = p$. This implies that $f = 1$ or $\frac{p-1}{p+1}$. The former solution contradicts to the original assumption, while the latter one contradicts to $\gcd(\frac{K-2}{2}, d) = 1$. All of above promise that $\delta_M(\tau \rightarrow \tau'; \mathbf{A}) = 0$. Therefore, $\theta_M(\tau_1, \dots, \tau_M; \mathbf{A})$ is a constant of τ_1, \dots, τ_M . Hence, $\{\mathbf{s}_1, \dots, \mathbf{s}_M\}$ is SI. This completes the inductive step. \blacksquare

D. The case of $\gamma = K - 1, K - 2, K - 3$

For larger γ , we first rewrite (15) as

$$\mathbb{E}(LR_1 + \dots + LR_M) = \sum_{i=1}^M Lf_i - \sum_{i=1}^M \frac{i \theta_i(\tau_1, \dots, \tau_M; \mathbf{A}) \theta_{\geq \gamma+1-i}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B})}{L},$$

where $\theta_{\geq j}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B}) := \sum_{k=j}^{K-M} \theta_k(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B})$. By the same argument in previous subsections, we obtain the following results in parallel with Theorems 16, 17 and 18. The proof is identical as before and is omitted here.

Theorem 19. *If a set of K binary sequences is TI with MPR capability $K - 1$, then this sequence set is SI.*

Theorem 20. *Let \mathcal{S} be a set of K binary sequences with the same duty factor $f = \frac{n}{d} \neq 0, 1$, which is TI with MPR capability γ .*

- (a) ($\gamma = K - 2$.) \mathcal{S} is SI if $\gcd(K - 2, d) = 1$.
- (b) ($\gamma = K - 3$.) \mathcal{S} is SI if (i) $K - 3$ is prime, and (ii) $\gcd(\frac{K-2}{2}, d) = 1$.

VIII. CONCLUSION

In this paper, considering the MPR capability γ we investigate TI sequences, which produce the invariant throughput for any relative shifts. Only one previous known result on TI sequences is that SI sequences must be TI for $\gamma = 1$ [6]. Considering some specific form of duty factors, this paper obtains that the length of TI sequences must be exponential in the number of users for any γ , and proves that some known constructions of SI sequences can be used to design optimal TI sequences for any γ . In addition, we explore the bit structure of TI sequences by showing that they must be pairwise SI for any γ , and further be SI in many specific cases. This tends to indicate that there are no shorter solutions to the TI problems than SI sequences. To our knowledge, the existence of TI sequences which are not SI is still unknown. Another aspect is to apply some known shorter sequences, such as wobbling sequences or CRT sequences, to promise a quasi-TI performance for MPR, which is of more practical interests in a realistic system. We leave these problems to the interested readers. Furthermore, having understood the fundamental behavior of MPR on TI sequences, we propose a practical identification and decoding mechanism, by incorporating packet header, RS code, and advanced PHY-layer blind packet separation algorithms.

APPENDIX

A. Proof of (8)

We first construct the following four binary sequences:

- (i) $\mathbf{s}_{\alpha_1}(t) = 1$ if and only if $s_1(t + \tau_1) + s_2(t + \tau_2) = 1$ for each $0 \leq t \leq L - 1$;
- (ii) $\mathbf{s}_{\alpha_2}(t) = 1$ if and only if $s_1(t + \tau_1) = s_2(t + \tau_2) = 1$ for each $0 \leq t \leq L - 1$;
- (iii) $\mathbf{s}_{\beta_1}(t) = 1$ if and only if $\sum_{i=3}^K s_i(t + \tau_i^*) \leq \gamma - 1$ for each $0 \leq t \leq L - 1$.
- (iv) $\mathbf{s}_{\beta_2}(t) = 1$ if and only if $\sum_{i=3}^K s_i(t + \tau_i^*) \leq \gamma - 2$ for each $0 \leq t \leq L - 1$.

It is obvious that

$$\begin{aligned} N(1|\mathbf{s}_{\alpha_1}) &= \theta_1(\tau_1, \tau_2; \mathbf{A}), & N(1|\mathbf{s}_{\alpha_2}) &= \theta_2(\tau_1, \tau_2; \mathbf{A}), \\ N(1|\mathbf{s}_{\beta_1}) &= \theta_{\leq \gamma-1}(\tau_3^*, \dots, \tau_K^*; \mathbf{B}), & N(1|\mathbf{s}_{\beta_2}) &= \theta_{\leq \gamma-2}(\tau_3^*, \dots, \tau_K^*; \mathbf{B}). \end{aligned}$$

Then by (2) we have

$$\sum_{\tau_{\alpha_1}=0}^{L-1} \sum_{\tau_{\beta_1}=0}^{L-1} N(1, 1|\mathbf{s}_{\alpha_1}^{(\tau_{\alpha_1})}, \mathbf{s}_{\beta_1}^{(\tau_{\beta_1})}) = LN(1|\mathbf{s}_{\alpha_1})N(1|\mathbf{s}_{\beta_1}).$$

The left-hand-side in the above identity is equal to $L^2 \mathbb{E}(T_1(\tau_1, \tau_2))$. Then we have $\mathbb{E}(T_1(\tau_1, \tau_2)) = \theta_1(\tau_1, \tau_2; \mathbf{A})\theta_{\leq \gamma-1}(\tau_3^*, \dots, \tau_K^*; \mathbf{B})/L$.

Similarly, we have

$$\sum_{\tau_{\alpha_2}=0}^{L-1} \sum_{\tau_{\beta_2}=0}^{L-1} N(1, 1|\mathbf{s}_{\alpha_2}^{(\tau_{\alpha_2})}, \mathbf{s}_{\beta_2}^{(\tau_{\beta_2})}) = LN(1|\mathbf{s}_{\alpha_2})N(1|\mathbf{s}_{\beta_2}),$$

and thus $\mathbb{E}(T_2(\tau_1, \tau_2)) = \theta_2(\tau_1, \tau_2; \mathbf{A})\theta_{\leq \gamma-2}(\tau_3^*, \dots, \tau_K^*; \mathbf{B})/L$.

B. Proof of (16) \Rightarrow (14)

For convenience, in this proof $\delta_M(\tau \rightarrow \tau'; \mathbf{A})$, $\theta_k(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B})$ and $\theta_{\leq k}(\tau_{M+1}^*, \dots, \tau_K^*; \mathbf{B})$ will be abbreviated as δ_M , θ_k and $\theta_{\leq k}$, respectively. By Lemma 14,

$$\begin{aligned} 0 &= \delta_M \sum_{i=1}^M (-1)^{M-i} \binom{M-1}{i-1} \theta_{\leq \gamma-i} \\ &= \delta_M (-1)^{M-1} \sum_{i=1}^M (-1)^{i-1} \binom{M-1}{i-1} \theta_{\leq \gamma-i} \\ &= \delta_M (-1)^{M-1} \sum_{i=1}^{M-1} (-1)^{i-1} \mathbf{A}_i (\theta_{\leq \gamma-i} - \theta_{\leq \gamma-i-1}) + \delta_M \mathbf{B} \theta_{\leq \gamma-M}, \end{aligned}$$

where

$$\mathbf{A}_i = \sum_{j=1}^i (-1)^{j-1} \binom{M-1}{i-j}, \quad \mathbf{B} = \sum_{j=0}^{M-1} (-1)^j \binom{M-1}{M-1-j}.$$

Binomial recursive formula states that

$$\binom{n}{m} - \binom{n-1}{m-1} = \binom{n-1}{m}, \forall 1 \leq m \leq n.$$

By replacing $\binom{M-1}{0}$ by $\binom{M-2}{0}$, we have $\mathbf{A}_i = \binom{M-2}{i-1}$. In addition, $\mathbf{B} = 0$ by binomial theorem.

The above equation is therefore

$$\delta_M \sum_{i=1}^{M-1} (-1)^{M-i} \binom{M-2}{i-1} (\theta_{\leq \gamma-i} - \theta_{\leq \gamma-i-1}) = \delta_M \sum_{i=1}^{M-1} (-1)^{M-i} \binom{M-2}{i-1} \theta_{\gamma-i}.$$

REFERENCES

- [1] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 31, no. 2, pp. 192–204, Mar. 1985.
- [2] N. Q. A. L. Györfi, and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 940–949, May 1992.
- [3] L. Györfi and I. Vajda, "Construction of protocol sequences for multiple-access collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 1762–1765, Sep. 1993.
- [4] W. S. Wong, "New protocol sequences for random access channels without feedback," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2060–2071, Jun. 2007.
- [5] C. S. Chen, W. S. Wong, and Y.-Q. Song, "Constructions of robust protocol sequences for wireless sensor and ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 57, no. 5, pp. 3053–3063, 2008.
- [6] K. W. Shum, C. S. Chen, C. W. Sung, and W. S. Wong, "Shift-invariant protocol sequences for the collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3312–3322, Jul. 2009.
- [7] K. W. Shum and W. S. Wong, "Construction and applications of CRT sequences," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5780–5795, Nov. 2010.
- [8] S. Ghez, S. Verdú, and S. C. Schwartz, "Stability properties of slotted ALOHA with multipacket reception capability," *IEEE Trans. Autom. Control*, vol. 33, no. 7, pp. 640–649, 1988.
- [9] Y. Zhang, P. Zheng, and S. Liew, "How does multiple-packet reception capability scale the performance of wireless local area networks?" *IEEE Trans. Mobile Comput.*, vol. 8, no. 7, pp. 923–935, Jul. 2009.
- [10] F. Babich and M. Comisso, "Theoretical analysis of asynchronous multi-packet reception in 802.11 networks," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1782–1794, Jun. 2010.
- [11] A. I. B and T. G. Venkatesh, "Order statistics based analysis of pure ALOHA in channels with multipacket reception," *IEEE Commun. Lett.*, vol. 17, no. 10, pp. 2012–2015, Oct. 2013.
- [12] A. Mukhopadhyay, N. Mehta, and V. Srinivasan, "Design and analysis of an acknowledgment-aware asynchronous MPR MAC protocol for distributed WLANs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2068–2079, May 2013.
- [13] D. Chan, T. Berger, and L. Tong, "Carrier sense multiple access communications on multipacket reception channels: Theory and applications to IEEE 802.11 wireless networks," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 266–278, Jan. 2013.
- [14] S. Tinguely, M. Rezaeian, and A. J. Grant, "The collision channel with recovery," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3631–3638, Oct. 2005.
- [15] Y. Zhang, K. W. Shum, and W. S. Wong, "On pairwise shift-invariant protocol sequences," *IEEE Commun. Lett.*, vol. 13, no. 6, pp. 453–455, Jun. 2009.

- [16] V. C. da Rocha, Jr., "Protocol sequences for collision channel without feedback," *IEE Electron. Lett.*, vol. 36, no. 24, pp. 2010–2012, Nov. 2000.
- [17] S. Talwar, M. Viberg, and A. Paulraj, "Blind separation of synchronous co-channel digital signals using an antenna array, part I: Algorithms," *IEEE Trans. Signal Processing*, vol. 44, no. 5, pp. 1184–1197, May 1996.
- [18] A. van der Veen, "Algebraic methods for deterministic blind beamforming," *Proc. IEEE*, vol. 86, pp. 1987–2008, Oct. 1998.
- [19] L. Tong, Q. Zhao, and G. Mergen, "Multipacket reception in random access wireless networks: From signal processing to optimal medium access control," *IEEE Commun. Mag.*, pp. 108–112, Nov. 2001.